**AFFIDAVIT OF SPECIAL AGENT JASON D. COSTELLO IN SUPPORT OF AN APPLICATION FOR SEARCH WARRANTS**

I, Jason D. Costello, having been sworn, state:

***INTRODUCTION AND AGENT BACKGROUND***

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"). I joined the FBI in July 2004. From December 2004 through July 2010, I was assigned to the Violent Crimes Task Force of the FBI's Boston Division at Boston, Massachusetts. Since August 2010, I have been assigned to the Organized Crime Task Force ("OCTF") of the FBI's Boston Division. My primary duties on the OCTF include the investigation of Eurasian criminal enterprises, specifically Balkan organizations.

2. In addition to my 17 weeks of basic investigative training at the FBI Academy in Quantico, Virginia, I have received training on investigating technology-based and cyber-based crimes, including the following: yearly computer based training on basic cybercrime topics and basic cellular technology exploitation; in-service trainings on advanced cellular technology exploitation; and a conference on Bulgarian and Romanian cyber organized crime and the various technology-based and cyber-based crimes attributable to those groups.

3. As an FBI Special Agent, I have utilized various investigatory tools and techniques, including confidential informants, cooperating witnesses, undercover agents, physical surveillance, search warrants, telephone toll analysis, court-authorized electronic surveillance, grand jury investigations, and witness interviews. I am familiar with the benefits and limitations of these techniques. I have previously submitted affidavits in support of search and arrest warrants in the United States District Court for the District of Massachusetts.

4. I am currently investigating LUDEMIS HORNEA a/k/a Antonio Scapesia and others for the crimes of conspiracy to use counterfeit access devices in violation of 18 U.S.C.

§ 1029(b)(2) and possession of device making equipment in violation of 18 U.S.C. § 1029(a)(4) (hereinafter, the "Target Offenses").

5. This affidavit is being submitted in support of an application for a warrant, under 18 U.S.C. § 2703(a) and Rule 41 of the Federal Rules of Criminal Procedure, to search and seize the Facebook accounts identified as follows, and other data associated with those accounts:

a. by the Facebook user identification ("UID") 100004369117504 and vanity uniform resource locator ("URL") of www.facebook.com/ludemis.hornea ("the LUDEMIS HORNEA Facebook Account")

b. by the Facebook UID 100004495770593 (the "CONSTANTIN HORNEA Facebook Account") and URL www.facebook.com/profile.php?id=100004495770593;

c. by the Facebook UID 100000309485302 and Vanity URL www.facebook.com/claudio.florea (the "CLAUDIU Facebook Account");

d. by the Facebook UID 100006871982416 and Vanity URL www.facebook.com/ludy.ludemis.9 ("LUDY LUDEMIS Facebook Account");

e. by the Facebook UID 100004680823873 and Vanity URL www.facebook.com/stau.cavulturupestaca ("SUEDIN CHICIU Facebook Account");

f. by the Facebook UID 100001843243076 and Vanity URL www.facebook.com/chdheu ("BADEA Facebook Account"); and

g. by the Facebook UID 100003187275603 and Vanity URL www.facebook.com/birgu.boss ("BIRGU BOSS Facebook Account," collectively the "Facebook Accounts").

The Facebook Accounts are described in Attachment A. There is probable cause to believe that the Facebook Accounts contain fruits, evidence, and instrumentalities of the crimes listed in

paragraph 4, as described in Attachment C.

6. The Facebook Accounts and relevant data are maintained by Facebook, Inc., which, government databases indicate, accepts service of process at 1601 Willow Road, Menlo Park, CA 94025 and via its law enforcement portal at www.facebook.com/records.

7. I also submit this affidavit in support of an application for a warrant under 18 U.S.C. § 2703 (a) and Rule 41 of the Federal Rules of Criminal Procedure to search and seize records and data from the e-mail accounts identified as ludy.ludemis@gmail.com and ludemis.hornea@gmail.com (the "Target Google Accounts") (as described in Attachment B). There is probable cause to believe that the Target Google Accounts contain evidence, fruits, and instrumentalities of the crimes identified above, as described in Attachment D.

8. Based on the e-mail addresses' domain names, I have probable cause to believe that the Target Google Accounts and relevant data are maintained by Google, which, government databases indicate, accepts service of process at: USLawEnforcement@google.com and via its law enforcement portal at: https://support.google.com/legal-investigations/contact/LERS as described in Attachment B.

9. The facts in this affidavit come from my personal observations and review of records, my training and experience, and information obtained from other agents and witnesses. This affidavit includes only those facts I believe are necessary to establish probable cause and does not include all of the facts uncovered during the investigation.

***TECHNICAL BACKGROUND- FACEBOOK***

10. Facebook is an online social networking service accessible at the website www.facebook.com or via an application ("app") that can be installed on computer equipment, including a tablet or a cell phone. Facebook allows users to create profiles and share personal

and biographical information; share content and media, including by uploading photographs and videos and sending links to other content; and communicate with other users in a variety of ways, from public discussions to private messaging.

11. When a user creates a Facebook account, they provide Facebook with information to begin building their online Facebook profile, selecting a Display Name and providing an email address and/or telephone number that will be associated with the account. The user may choose to upload photographs, go with a default Uniform Resource Locator (URL) or create a customized one known as a Vanity URL and provide other information as well for the "About Me" section of the page, including basic information such as where the user lives, works, and attends/attended school. This information is then displayed on the user's page. The user may also provide Facebook with other contact information, such as additional phone numbers and email addresses. In addition, Facebook captures certain basic information about the new account, including the registration date and the IP address used to create the account. Further, Facebook assigns a unique numerical identifier to the account called a Facebook User Identification (UID).

12. Facebook users can continually build their online profile, and in my training and experience it is common for users to add and edit biographical information – for instance by updating on a new job or changing a "relationship status" to reflect changes in their life. Facebook actively prompts users to provide or confirm information, for instance by asking the user to confirm that they live in a particular city if other information in the profile or the majority of conflicts suggests that they might live in that city. As a result, Facebook users typically provide a significant amount of biographical information.

13. Facebook also encourages users to form connections with other users on the site,

most fundamentally by allowing users to connect as "Friends." A Facebook user creates a "Friend" connection by inviting another Facebook user to confirm that they are "Friends." When the request is accepted, the connection is created. Facebook also prompts users to connect with other users when they share common connections.

14. Facebook offers users a variety of privacy settings. The Display Name and the Profile Picture and Cover Photo are publicly visible to anyone that visits the page, and are generally searchable unless a user has selected not to be searchable. Facebook users can keep their entire profile open publicly as well, which allows anyone to view all of the content and information on their profile. The Facebook user can make the content of their page visible only to users that have been confirmed as "Friends," or visible to both "Friends" and anyone confirmed as a "Friend" of their "Friend" (exponentially increasing the number of people that can view that content). Further, Facebook users can create lists within their "Friends" and allow certain content to be viewed only by subgroups of their Friends (e.g. "Friends" designated as "Work Friends," or "Family").

15. The first page of every Facebook account displays a Display Name and the space for both a "Profile Picture" and a "Cover Photo." Facebook users can post additional photos or even entire photo albums. In my training and experience, most Facebook users build their profiles by uploading and changing photographs on their account. Many users own mobile devices that contain cameras, and it is common for mobile cameras and popular camera mobile applications (such as Instagram, an application owned by Facebook) to prompt users to post pictures to their Facebook accounts after a photo is taken.

16. Facebook users have the ability to indicate that other people who appear in their photos are also on Facebook by "tagging" them in the photograph using their Display Name. A

Facebook user can adjust their privacy settings to require that they confirm a tag before it can be successfully applied.

17. Facebook users can comment on their own photographs and other users' photographs or indicate that they "Like" a particular image.

18. In addition to photographs, Facebook users can write messages, or "Status Updates," on their page. This was traditionally referred to as their "wall" or a "wall post," and is now called a "Timeline." Unless the user actively deletes them, older postings may be viewable on the users' account by looking back through the "Timeline." Facebook users can also add "life events" with a date on their "Timeline," such as the date they began a particular job or were married. As with photographs and other content, the user can select who can view their posts – allowing them to be visible publicly (the default) or limiting their display to only a selected group of individuals.

19. Facebook users can also send private messages to other Facebook users, as well as to email addresses. These can be directed to individuals or initiator-defined groups. These messages are only viewable by the recipient(s). For mobile device users, Facebook created the Facebook Messenger application to perform this function. The Facebook Messenger application allows users to send text messages, audio messages, photos and short videos to other users. The Facebook Messenger application also allows users to place voice calls to other users similar to standard telephone calling.

20. Facebook users can also create or join "Groups" of other users. Facebook Groups are used by a variety of communities and small groups and are a tool to communicate and share content.

21. Facebook also allows public figures, businesses, organizations, and other entities

to create Facebook Pages. Facebook users can become "Fans" of a Facebook Page.

22. Facebook users provide information about their physical location in different ways through their use of Facebook. As described above, Facebook users may affirmatively state their current address and their hometown. Facebook users may also post Status Updates that discuss where they are, who they are with, and what they are doing. Facebook users who are using a mobile device running the Facebook application may also be able to "Check In" to a location using a feature called "Facebook Places" if the location or establishment from which they are posting offers this feature. The check-in feature allows Facebook users to connect with other users, or "Friends," that are at or near the same location. In addition, Facebook collects other locational information regarding its users, such as the IP address for the device each time the user logs into the site.

23. While it is free to create a profile and use Facebook, Facebook does collect payment information for some uses. Companies that use Facebook can purchase advertisements and sponsored posts. Individual users can use Facebook Marketplace, an online classified service, to sell or purchase items. Facebook users can also purchase games and software applications, and related real or virtual products. Facebook users can also purchase "Facebook Credits" that can then be used for games and application purchases.

24. Facebook encourages connectivity and sharing, and numerous websites now allow users to access services or login to their pages through their Facebook account. In addition, many websites allow users to use Facebook to indicate that the user "Likes" the website, product, or affiliated group. Based on my training, I understand that Facebook also often obtains information regarding other internet activity by its users, even when that user has not actively logged in or affirmatively selected the "Like" button.

25. Facebook was founded in 2004 and has continually evolved, adding different types of services. In 2012, Facebook announced that it had grown to have more than 1 billion active users.

## *TECHNICAL BACKGROUND-GOOGLE*

26. In my training and experience and through discussions with other agents, I have learned that e-mail hosting companies, such as Google, maintain computer servers connected to the Internet. Their customers use those computers to send e-mail on the Internet.

27. Customers can access their accounts on Google's e-mail servers from any computer connected to the Internet. In addition, Google has storage capacity that allows customers to store opened incoming mail and sent mail indefinitely if they choose, subject to a maximum size limit.

28. E-mail providers also typically maintain electronic records relating to their customers. These records include account application information, account access information, and e-mail transaction information.

## *PROBABLE CAUSE*

### Probable Cause That LUDEMIS HORNEA and Others Committed the Target Offenses

29. On February 1, 2016, Braintree Police received information from Bank of America that a skimming device was discovered on a Bank of America ATM located at 400 Franklin Street, Braintree, Massachusetts (hereinafter, "the Braintree ATM"), which consisted of a concealed magnetic strip reader/recorder placed over the card reader controlling access to the vestibule door and a concealed a micro-camera adhered to the ATM pointed at the number

keypad.[1] Bank of America security had reviewed security video footage, identified the male party who had installed the camera portion of the skimming device, and supplied photographs of that person to Braintree Police. I have reviewed the security video footage of the person who installed the camera portion of the skimming device and identified that person as HORNEA.

30. That day (February 1, 2016), at approximately 8:00 p.m., Braintree Police detectives saw a male approaching the Braintree ATM (hereinafter, "the suspect") who they believed resembled the person from the security photographs. The suspect was wearing a black jacket, black jeans with a striped pattern, sunglasses and a hood over his head. The suspect walked up to the Braintree ATM and around to the side, where the vestibule door was located. As a detective pulled up, the suspect was still standing by the vestibule door, with his hands and attention focused on the area of the door's card reader. The suspect then looked over at the detective's car and started walking away from the door. The detective, who was wearing an external vest with "police" written on it, got out of his car and started walking toward the suspect. The suspect started walking away briskly. The detective identified himself as police and told the suspect to stop. Instead, the suspect started running away through the parking lot and down Franklin Street. The detective followed on foot while another detective attempted to

[1] ATM skimming is described as surreptitiously obtaining the debit card numbers and corresponding personal identification numbers (PINs) of bank customers utilizing an ATM. I am generally familiar with skimming devices. The skimming devices, such as the one described herein, often consist of two parts, one to capture and record the account information contained in the magnetic strip of a card and the other to capture and record the user's PIN. The former is often made to look like the legitimate card access slot, either on an exterior access control or on the ATM itself and does not interfere with the card access functions. The latter is usually a separate pinhole camera device that is discreetly hidden on the ATM or near it in a location from which the customer's input on the ATM keyboard can be observed. Each piece of information is generally stored on the separate part that recorded it; the information is typically downloaded to a computer and combined. In order to access the accounts illegally, the account information is burned to a cloned card. The account owner's PIN and the cloned card are then used to withdraw money, typically the maximum withdrawal amount, from the account owner's account.

cut the suspect off in a car.

31. The suspect ran into a parking lot and got into the passenger seat of a Volkswagen, which fled at high rate of speed. The car was gray with black rims and there was a female in the rear passenger seat. Braintree Police radioed this information to surrounding cities and towns.

32. Approximately 10 minutes later, a Massachusetts State Police (MSP) trooper spotted the Volkswagen traveling extremely fast on Route 93 South at the intersection with Route 95 North. The trooper could not catch the car but reported that it crossed four lanes and exited at that the University Avenue ramp in Westwood.

33. Westwood Police officers and MSP troopers began searching the University Avenue area for the Volkswagen. About 20 minutes later the empty Volkswagen was located parked in the lot of Lifetime Fitness at 44 Harvard Street, which is off University Avenue. Westwood Police officers and MSP troopers on foot and in cars began searching the area for the three occupants of the Volkswagen. Officers were checking the University Station shops when they saw the suspect exit the nearby Petsmart store. The officers approached but the suspect fled. After a foot pursuit and struggle to avoid being restrained, officers used tasers to subdue and then arrested the suspect. The suspect identified himself as "Antonio Scapescia" and officers found a photo identification card, appearing to be issued by the Italian government, in that name in his wallet. When Braintree Police detectives arrived they confirmed that "Scapescia" was the suspect they saw outside the Braintree ATM and who fled into the Volkswagen.

34. Officers returned to the Petsmart store. An employee informed them that a male and female, who had originally entered the store with the individual who ran from police

("Scapescia"), were still in the store. Officers located both shortly thereafter looking at pet supplies. Officers asked both for identification. The male produced a non-government issued photo identification card in the name of "Nutu Popescu". The female did not have identification but identified herself as ISABELA FLOREA. Both were detained pending identification by Braintree Police detectives. The employee told officers that the three had entered the store together and asked the store manager to call a cab for them in an excited fashion. When they learned that a cab would take 20 minutes to arrive, they asked the employee if he could give them a lift. The keys to the Volkswagen were found in "Popescu's" pocket and he admitted, after having received *Miranda* warnings, that he had driven the Volkswagen and that FLOREA was the woman in the backseat.

35. FLOREA, who was a juvenile at the time (she turned eighteen on March 19, 2016), had a default warrant out of Middlesex County Juvenile Court for previous skimming cases and was arrested on that warrant.[2] "Scapescia" and "Popescu" were placed under arrest and transported to the Braintree Police Department to be charged with state offenses, including identity fraud, breaking into a depository, defacing property, and conspiracy. Sometime after both men were fingerprinted during booking, Braintree Police were notified by an automated response from the FBI's Criminal Justice Information Systems (CJIS) Division that based on fingerprint records "Scapescia" is actually HORNEA and "Popescu" is actually ION BONCULESCU. HORNEA continues to be held in custody by the Norfolk County Sherriff's

[2] FLOREA was arrested and charged by the Waltham, Massachusetts Police on August 6, 2015, after she was caught removing a skimming device from a Bank of America ATM machine in that town. On November 17, 2015, Concord, Massachusetts Police recovered a skimming device from a Bank of America ATM machine in that town. Review of the security video showed that FLOREA had placed the camera portion of the device on the machine. Concord Police later charged FLOREA with the attempted skim. These charges were the basis for the default warrant on which Florea was arrested on the night of February 1, 2016.

Department on the state case. BONCULESCU was released after posting $35,000 cash bail.

36. Following his arrest and after receiving *Miranda* warnings, HORNEA gave a video-taped interview, which I have reviewed. HORNEA, who continued to identify himself as "Scapescia" during the interview, advised that he was part of the Roma or "Gypsy" community. He admitted to having placed the skimming device (both parts) on the Braintree ATM on February 1, 2016, for the purpose of capturing both bank customer debit card numbers and their corresponding PINs. HORNEA admitted that he did this so that the cards could later be cloned by his co-conspirators and used to make unauthorized withdrawals out of the bank customer accounts. HORNEA was returning to the Braintree ATM to retrieve the skimming device, which he believed would contain captured card numbers and PINs, when Braintree Police detectives approached him and he fled with the help of his driver. HORNEA did not identify BONCULESCU as the driver by name, but instead as the "skinny" guy he was arrested with. HORNEA had just removed the magnetic strip reader/recorder portion of the device off of the vestibule door card reader, which he referred to as the "square" in reference to its shape, when detectives approached him. He advised that he threw it under a parked car as he ran. HORNEA had not yet made it inside the Braintree ATM vestibule to recover the camera.[3]

37. HORNEA admitted that he had installed and removed the same skimming device (both parts) from the Braintree ATM on the two or three days prior to February 1, 2016,[4] at the

[3] The magnetic strip reader/recorder portion of the device was later recovered by Braintree Police and entered into their evidence room. The camera portion of the device was recovered by Bank of America security personnel after Braintree Police pursued HORNEA out of the area. The camera was subsequently turned over to the affiant to be entered into evidence at FBI Boston.

[4] I have reviewed Bank of America security video footage from the Braintree ATM on January 29, 30 and 31, 2016, which shows a male who appears to be HORNEA installing and

direction of the "mechanic", whom HORNEA identified as an Albanian (non-Roma) male by the name of "Entes Mustafa". HORNEA explained that after removing the skimming device each day, he and his driver (BONCULESCU) travelled to New York where the skimming device was provided to Mustafa, who extracted the captured card numbers and PINs from the skimming device and recharged the batteries. Mustafa then returned the skimming device to HORNEA who, with his driver, returned to Massachusetts and installed it on the Braintree ATM for another day of capturing card numbers and PINs. HORNEA said that, had he not been arrested, he would have returned to New York and again given the skimming device to Mustafa. HORNEA expected that Mustafa would have provided HORNEA with cloned debit cards so that he could make cash withdrawals.

38. During the interview, HORNEA explained that Mustafa provided HORNEA with the skimming device and directed him to the Braintree ATM. HORNEA also advised that Mustafa paired HORNEA together with his driver (BONCULESCU). HORNEA also explained that there are other mechanics and that there was a "boss" over "everything," which I believe referred to organized ATM skimming conducted by individuals, such as HORNEA, from the Roma community.

39. HORNEA was in possession of a debit card in the name of CONSTANTIN HORNEA. HORNEA explained that CONSTANTIN was a friend who lent him his debit card. HORNEA denied having stayed at a hotel or motel in or near Massachusetts in the days leading up to his arrest stating that it was too dangerous for him to stay somewhere because pictures of him may have been circulated by law enforcement. HORNEA claimed that he and BONCULESCU slept in the car when needed as they travelled back and forth to New York.

---

removing the camera portion of the device, as he did on February 1, 2016. In the security video, HORNEA appears to be wearing the same jacket and hat that he was wearing when arrested.

40. HORNEA identified FLOREA as his girlfriend. HORNEA advised that he and FLOREA had seven month-old child together and that FLOREA was pregnant with their second child. HORNEA denied that FLOREA was involved with the skimming incident for which he and BONCULESCU were arrested for. HORNEA claimed that FLOREA may have been staying in a hotel or motel in the area but that he did not know where. HORNEA acknowledged that FLOREA had a prior arrest for skimming. HORNEA indicated that he was aware that FLOREA possessed a "square" around the time of her arrest but claimed ignorance of her skimming activities. HORNEA told detectives that FLOREA did not have a phone.

**Probable Cause that HORNEA Possessed the Device and Used It During the Commission of the Target Offenses**

41. HORNEA had an iPhone 6s (hereinafter, the "Device") on his person at the time of arrest. The Device was seized and placed with HORNEA's personal property bag upon booking. At his request, HORNEA was allowed supervised access to the Device during the video-taped interview in an effort to provide information to detectives. HORNEA utilized a six-digit pass code he knew from memory to unlock the Device. When HORNEA was transferred from Braintree Police custody to the custody of the Norfolk County Sheriff's Department ("NCSD"), the Device was placed into storage by the NCSD at 200 West Street, Dedham, Massachusetts.

42. During the interview HORNEA showed detectives an English-language SMS text message exchange between he and phone number 646-724-2565, stored as a contact on the Device as "Gggg". HORNEA identified the contact ("Gggg") as Mustafa.

43. During the interview the Device continued to receive incoming calls and/or messages which were not answered. Some or all of these incoming calls and/or messages appeared on the Device's lock screen under the stored contact name of "Faby Fabritio".

Detectives observed this and asked HORNEA who "Faby Fabritio" was. HORNEA advised that "Faby Fabritio" was his brother's Facebook account but that it was likely HORNEA's mother who was trying to contact him through it. HORNEA advised detectives that he used Facebook Messenger to communicate with people. HORNEA told detectives that his phone number was 347-255-8248.

44. On June 8, 2016, the Court authorized the FBI to seize and search the Device (see 16-MJ-1026-DLC). On June 9, 2016, the FBI seized the Device from the NCSD. The Device was then brought to the FBI's Boston office where it was entered as evidence and searched. The search of the Device showed that it was assigned phone number 347-255-8248 (i.e., HORNEA's number), that it bore IMEI 353265078119973 and that it was associated with IMSI 310260399833360.

45. The Device contained voluminous photographs and videos of HORNEA (including many "selfie" photos and videos), FLOREA, and a small child. In a SMS text message conversation translated from Italian to English between the Device and telephone number 347-827-6568, the user of 347-827-6568 (likely Florea) calls the user of the Device "my husband" and talks about their young child.[5] From this, I believe that HORNEA not only possessed the Device at the time of his arrest, but was also the user of the Device prior to his arrest.

46. The Device also contained two short "selfie" video clips of HORNEA smiling and posing in front of two police vehicles in a parking lot taken on the evening of January 30, 2016. The timestamp on the selfie videos indicates that they were taken approximately one hour before

[5] For this affidavit, I have relied on preliminary, draft translations by FBI-certified translators.

HORNEA removed the camera portion of the skimming device from the Braintree ATM on that day. HORNEA also appeared to be wearing the same jacket and hat in the selfie videos as he was in the security video.

47. The Device also contained numerous close-up photographs and videos of suspected skimming devices appearing to have been taken on various dates in January 2016. At this time, I do not know where HORNEA and the Device were when the photographs and videos were taken. The Device also contained a photograph of the card access reader on an ATM vestibule door, or possibly a skimming device installed over the actual card access reader, and a photograph of what appears to be the back of a skimming device, taken in December 2015.

48. The Device also had the application Skype installed. A review of that application showed that the name on the account was "Alex Velea," who I believe was a codename for HORNEA based on HORNEA's use of the Device. HORNEA/"Velea" had a total of six saved Skype contacts. Of these six, five appear to be Chinese women whose Skype profiles identify them as working for either custom plastic molding companies or electronics companies selling micro cameras or card readers, of the type found in ATM skimming devices, in China. HORNEA had recent chat exchanges with two of these contacts and appeared to have been shopping for both card readers and micro cameras in December 2015 and January 2016. In one of the chat exchanges HORNEA was told that payment to China would be made in the form of a Western Union wire transfer to Guangzhou, China.

49. I opened the Device's internet browser (Apple's Safari) and observed that there were six open pages or search terms entered: "attleboro motor inn"; "cinema Attleboro ma"; "fpispysource.com"; "ferrari ff for sale"; "ents mustafa"; and "cardreaderfactory.com". I have found that fpispysource.com is a New York based seller of spy equipment, such as micro

concealed cameras. Cardreaderfactory.com is an internationally based internet seller of micro magnetic stripe readers. I have also spoken with the Attleboro Motor Inn, which is located in Attleboro, Massachusetts, and found that according to their records HORNEA, under his alias "Antonio Scapescia," stayed there on the nights of January 28 and 29, 2016, which were the eve and first night of the Braintree ATM skimming incident.

50. Finally, the Device contained numerous photographs and videos of individuals believed to be HORNEA's relatives and associates. The settings of these photographs and videos include vehicles, in social clubs and at restaurants. As will be described in more detail later in this affidavit, I recognize some of these relatives and associates from security photographs provided to me by Bank of America of other skimming incidents and related "cash-outs" of cloned debit cards in Massachusetts.

**Probable Cause That the Target Google Accounts Contains Fruits, Evidence, or Instrumentalities of the Target Offenses**

51. The Device contained both the Google Mail and Google Maps applications. The Device had access to two Google email accounts: ludy.ludemis@gmail.com and ludemishornea@gmail.com. At the time of the search the Device's organic mail application was signed into ludemishornea@gmail.com. Emails visible on the Device while in airplane mode included correspondence from Apple indicating that the email was associated with the Device's Apple account. At the time of the search both the Google Mail and Google Maps applications were signed in to ludy.ludemis@gmail.com. Due to the Device being in airplane mode, emails in the Google Mail application were not visible. However, the application's icon indicated that

there were unread emails.[6] Due to the Device being in airplane mode, recent places were not visible. However, the Device was found to have stored on it approximately 21 saved "screen shots" from the navigation function of Google Maps application. These screen shots showed mostly Bank of America ATMs located in Massachusetts, Connecticut, New York and Pennsylvania.

52. The saved screen shots from the Google Maps application showed the local time of the Device when the screen shot was saved and the address and estimated navigation time to the ATM. Estimated navigation times were shown as either based on walking or driving. The walking times ranged from one minute to three minutes, suggesting the Device was in use in close proximity to the ATM when the Google Maps screen shot was saved. The driving times were generally several hours, suggesting the Device was being used to navigate for a long trip or in planning a trip.

53. On the night of January 3 and morning of January 4, 2016, Google Maps screen shots were created of Bank of America ATMs in Whately, Massachusetts (10:43 PM, one minute walk); Amherst, Massachusetts (11:03 PM, one minute walk); Hadley, Massachusetts (11:06 PM, two minute walk); West Springfield, Massachusetts (11:56 PM, one minute walk), Westfield, Massachusetts (12:06 AM, three minute walk) and Norwalk, Connecticut (2:11 AM, 17 minute drive). I have obtained security video from Bank of America from the Whately and West Springfield ATMs on the night of January 3, 2016.[7] The video shows that at

[6] I believe that those emails may include information from Facebook because I am aware that Facebook messenger may be set to notify the user of updates in the user's designated, usually primary, email account.

[7] Security video for the remaining ATMs was no longer available when I requested it, except for the Amherst ATM, for which there were no activity or no obvious suspects.

approximately 10:43 PM, a man who I believe was HORNEA's brother, CONSTANTIN DENIS HORNEA (hereinafter "CONSTANTIN HORNEA"), entered the Whately ATM kiosk and possibly inserted a card into the machine. At approximately 11:55 PM, CONSTANTIN HORNEA entered the West Springfield ATM and did the same.[8] The geographical and chronological progression of the saved Google Maps screen shots and CONSTANTIN HORNEA's corresponding appearance in security video suggests that HORNEA, CONSTANTIN HORNEA and the Device travelled together to these locations, likely, as described below, to scout locations for skimming.

54. On January 7, 2016 (four days later), the Whately ATM was the site of an attempted skim. On that day Bank of America security video shows a male, who I believe was HORNEA, install the camera portion of a skimming device. The device was detected by a customer later that day, however, and recovered by local police prior to HORNEA or others returning to remove it.[9]

55. At approximately 1:26 PM on January 29, 2016, security video shows HORNEA installing the camera portion of skimming device on the Braintree ATM. The Device contained a saved Google Map screen shot of the Bank of America ATM located at 620 Middle Street, Weymouth, Massachusetts. This screen shot appears to have been created at 1:41 PM and showed that the Device was located within a two minute walk of the Weymouth ATM at the time. Of note is that screen shot of the Weymouth ATM was saved, in the area of the ATM,

[8] I recognized CONSTANTIN from known photographs from the United States Customs and Border Protection, family photographs with HORNEA and others from the Device and from his many photographs posted to his public Facebook page of "Faby Fabritio".

[9] The device was submitted to a state crime laboratory for analysis. Based on a photograph, the camera portion appears to be of the same basic design as the one recovered from the Braintree ATM.

approximately 15 minutes after HORNEA departed the Braintree ATM. This is consistent with the time required to travel between the two locations. Later that night Google Maps screen shots were saved to the Device showing Bank of America ATMs located at 1 Scammell Street, Quincy, Massachusetts and 440 Hancock Street, Quincy, Massachusetts. The Scammell Street ATM was the site of a skimming incident that took place on January 16, 17, 18 and 20, 2016. The Weymouth and Hancock Street ATMs were the sites of corresponding unauthorized withdrawals conducted by HORNEA, CONSTANTIN HORNEA and others on January 22, 2016. I believe that the saved screen shots indicate that HORNEA's Google account, specifically Google Maps, was again being used to search for, navigate to and/or store the locations for future reference in support of the Target Offenses.

56. The web history stored in the device shows that on various dates in January 2016, Google searches were conducted for such things as expensive cars, casino locations, "cardreaderfactory", casting or molding techniques, "atm skimming suspects" and hotel locations. I believe this activity is consistent with HORNEA using his Google account to search for items, places or tradecraft in connection with his commission of the Target Offenses. Furthermore, if the Device was signed in to his Google account at the time of those—or other searches—the Google account would have a record of them.

57. I am also aware that Facebook Messenger can be set to notify a user such as HORNEA of updates in a designated email account, such as the Google account. As a result, the Google accounts may contain additional information regarding the Facebook activity described below.

58. In my training and experience, the information stored in connection with an email account can indicate not simply who, but where a user has controlled it. This "user attribution"

evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, images sent with an e-mail (and the data associated with the foregoing, such as date, time, and .exif geolocation data) can indicate where a user was at a particular time. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crimes under investigation. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email), allowing investigators to identify other locations of skimming activity. Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

59. I am also aware that Google has a feature called Location History. According to Google's website, the feature "helps you get useful information – for example, automatic commute predictions, improved search results, by creating a private map of where you go with your logged in devices." Based on information already obtained from the Device, I believe that HORNEA was likely using this feature to locate skimming targets. To the extent HORNEA has used a logged-in device to access Google's services, there is probable cause to believe that Google will have a record of the location of that logged in device.

60. Other Google features, including Google Calendar, Google Maps, and Web History can also reflect geographic information for saved appointments, searches for directions,

and web navigation, which are all based on my training and experience common uses of Internet-based searches (for example, to locate a local restaurant, museum, or parking garage).

61. On July 20, 2016, the FBI submitted to Google a letter requesting under 18 U.S.C. § 2703(f) that the company preserve records associated with the Target Google Accounts for 90 days.

**Probable Cause That the Facebook Accounts Contain Fruits, Evidence, or Instrumentalities of the Target Offenses**

62. The Device contained the Facebook and Facebook Messenger applications. At the time of the search the Device was logged into to the Facebook account bearing Display Name "Dobrin Cristiano" with user identification (UID) 100004369117504 and vanity uniform resource locator (URL) of www.facebook.com/ludemis.hornea (the "LUDEMIS HORNEA Facebook Account"). I have reviewed the publicly available Facebook posts for this profile, including photographs, status updates and friends, and concluded that the likely user of this profile is in fact HORNEA. A review of the Facebook Messenger activity showed that HORNEA used this application regularly to communicate by both voice calls and text messages.[10] In this communications, HORNEA used Facebook to coordinate meetings with associates, send or receive wire transfer information or instructions to or from associates and send or receive telephone numbers to or from associates.

63. HORNEA, using the LUDEMIS HORNEA Facebook Account, frequently communicated via Facebook messenger, both voice calls and messages, with the Facebook

[10] Most, if not all, of the text communications occurred in Romanian, Roma or Italian. The FBI has performed preliminary translations of the Italian and Romanian communications. The FBI currently does not have Roma trained linguists. Where possible, and to the extent of their ability to partially understand Roma, which is similar to Romanian, Romanian linguists have translated portions of the Roma communications.

account bearing Display Name "Faby Fabritio" with UID 100004495770593 (the "CONSTANTIN HORNEA Facebook Account") and URL www.facebook.com/profile.php?id=100004495770593. I have reviewed the publicly available Facebook posts for this profile, including photographs, status updates and friends, and concluded that the likely user of this profile is CONSTANTIN HORNEA, HORNEA's brother, who was involved with HORNEA in scouting locations for skimming in Western Massachusetts in early January 2016 and in making unauthorized withdrawals in Quincy on January 22, 2016. In addition, as described below, HORNEA using the LUDEMIS HORNEA Facebook Account communicated with CONSTANTIN HORNEA using the LUDY LUDEMIS Facebook Account regarding the Target Offenses.

64. HORNEA, using the LUDEMIS HORNEA Facebook Account, frequently communicated via Facebook messenger, both voice calls and messages, with the Facebook account bearing Display Name "Claudio Mihaela Florea" with UID 100000309485302 and Vanity URL www.facebook.com/claudio.florea (the "CLAUDIU Facebook Account). I have reviewed the publicly available Facebook posts for this profile, including photographs, status updates and friends, and concluded that the likely user of this profile is CLAUDIU MIHAELA FLOREA[11] ("CLAUDIU"), who is the brother of FLOREA, HORNEA's wife and participant in the Braintree skimming incident.

65. HORNEA and CLAUDIU used their respective Facebook accounts to communicate regarding skimming. For example, on January 24, 2016, HORNEA sent a message to CLAUDIU that read "5966 fresh pond rd, Maspeth ny 11378". Based on my review of the

[11] I have noted that CLAUDIU has spelled his name "Claudio" on his Facebook Account. I know from my experience investigating Balkan groups that it is common for individuals to "Americanize" their names, often dropping or changing letters to facilitate pronunciation.

HORNEA/Mustafa text message exchange seized from the Device, I believe that the timing of this message corresponds to when HORNEA returned to New York after the Quincy skimming unauthorized withdrawals. On January 29, 2016, minutes after HORNEA installed the skimming device on the Braintree ATM, he sent CLAUDIU the message "Braintre MA", which I believe indicated to CLAUDIU the location of the latest skimming attempt. Later that afternoon HORNEA sent CLAUDIU the message "Attleboro motor inn", where HORNEA was staying under his "Scapescia" alias. CLAUDIU later checked-in to his own room at the Attleboro Motor Inn on the evening that this message was sent.

66. HORNEA, using the LUDEMIS HORNEA Facebook Account, frequently communicated via Facebook messenger, both voice calls and messages, with the Facebook account bearing Display Name "Ludy Ludemis" with UID 100006871982416 and Vanity URL www.facebook.com/ludy.ludemis.9 ("LUDY LUDEMIS Facebook Account"). I have reviewed the publicly available Facebook posts for this profile, to include photographs, status updates and friends, and concluded that the account was likely an older account belonging to HORNEA, as it had not been publicly updated since 2013. Based on the content of the messages translated so far, I believe that HORNEA gave CONSTANTIN HORNEA access to the LUDY LUDEMIS Facebook Account in order to communicate regarding the Target Offenses (HORNEA would not need to communicate with himself).

67. HORNEA and CONSTANTIN HORNEA had the following communications over their respective Facebook accounts.

- On January 27, 2015, starting at 10:28 PM, CONSTANTIN sent the following messages regarding what I believe were skimming proceeds:

"Code 5738568075 sent by Ilona Hornea. For Nicoleta Tudor the sum of 2050"; "Oh cousin, one of them got messed up, I'll go and take care of everything in the morning"; and "Code 0235817754, Maria Lazar is sending, Constantin Tudor is receiving, the sum of 2000";[12]

- On January 29, 2016, "Ludy Ludemis"/CONSTANTIN called HORNEA via Facebook messenger. Immediately after the call concluded HORNEA sent "Ludy Ludemis"/CONSTANTIN the message, "1 (646) 724-2565", which was the number belonging to "Mustafa".[13]

- On January 30, 2016, at approximately 7:48 PM, HORNEA sent "Ludy Ludemis"/CONSTANTIN the message "Done". This message was sent ten minutes after HORNEA was observed on security video removing the camera portion of the skimming device from the Braintree ATM on that day.

- On January 31, 2016, at approximately 10:38 AM, HORNEA sent "Ludy Ludemis"/CONSTANTIN the message "Use other door", which was sent ten minutes after HORNEA was observed on security video installing the camera portion of the skimming device on the Braintree ATM on that day.

68. HORNEA, using the LUDEMIS HORNEA Facebook Account, frequently

[12] I am aware that a money order was sent over Western Union to Romania with this information from Brooklyn, New York, at approximately 9:00 PM on January 27, 2015.

[13] Toll records show that immediately following that message, 347-898-1477 (CONSTANTIN) called Mustafa's number.

communicated via Facebook messenger, both voice calls and messages, with the Facebook account bearing Display Name "Suedin Chiciu" aka "Vulturu Versace" with UID 100004680823873 and Vanity URL www.facebook.com/stau.cavulturupestaca ("SUEDIN CHICIU Facebook Account"). I have reviewed the publicly available Facebook posts for this profile, to include photographs, status updates and friends, and concluded that the likely user of this profile is SUEDIN CHICIU, whom I have not further identified. However, HORNEA and SUEDIN CHICIU used their respective Facebook accounts to communicate about skimming. On January 30, 2016, HORNEA and CHICIU became Facebook friends. On January 31, 2016 (while the Braintree skimming was underway), at approximately 10:39 PM, HORNEA sent CHICIU the message "Use other door", which is the same message that he had sent to "Ludy Ludemis" one second earlier and likely referred to the door of an ATM. At approximately 1:07 PM, HORNEA sent CHICIU the message "50 South Ave, Burlington, MA", which is the address of a restaurant and was a likely meeting location.

69. HORNEA, using the LUDEMIS HORNEA Facebook Account, frequently communicated via Facebook messenger, both voice calls and messages, with the Facebook account bearing Display Name "Fernando Florin Badea" aka "Fernando Badea" with UID 100001843243076 and Vanity URL www.facebook.com/chdheu ("BADEA Facebook Account"). During his post-arrest interview, HORNEA advised that a "Fernando Florin Badea" was either a mechanic or worked for a mechanic ("BADEA"). HORNEA and BADEA used their respective Facebook accounts to communicate regarding the Target Offenses. For example, on January 24 and 25, 2016, BADEA provided HORNEA with passwords which were apparently not working. HORNEA then indicated "It's locked", which prompted calls via Facebook Messenger between the two. Later, more calls were exchanged and HORNEA then

sent what appeared to be a meeting address to BADEA. Based on the reference to "passwords," I believe that these communications referred to ATM skimmers known tradecraft of password protecting stolen data on the skimming devices and or computers used to process the data.

70. HORNEA, using the LUDEMIS HORNEA Facebook Account, frequently communicated via Facebook messenger, both voice calls and messages, with the Facebook account bearing Display Name "Birgu Boss" a/k/a "Birgazon Jakk" with UID 100003187275603 and Vanity URL www.facebook.com/birgu.boss ("BIRGU BOSS Facebook Account"). This account appears to have been deleted or deactivated sometime after preservation letters were served on Facebook. HORNEA communicated with the user of the BIRGU BOSS Facebook Account regarding the Target Offenses. For example, HORNEA sent to the BIRGU BOSS Facebook Account the confirmation codes, senders, recipients and amounts of Western Union and Money Gram wires, including the wire sent by CONSTANTIN HORNEA from New York to Romania previously discussed. The BIRGU BOSS Facebook Account sent return communications to HORNEA that the money was received and everything was okay. I believe that this money was likely obtained by skimming.

71. I believe that the requested information will either identify or confirm the users of the Facebook Accounts. In the case of Facebook Accounts whose users are identified, such as the LUDEMIS HORNEA Facebook Account (HORNEA), such information will corroborate HORNEA's participation. In the case of Facebook Accounts whose users are unidentified, such as the BIRGU BOSS Facebook Account, such information will identify additional participants in the Target Offenses. In addition, information about both activities and, crucially, locations and movement will confirm the skimming that occurred in Braintree, provide further information regarding other targets under investigation, such as Quincy and Whately, Massachusetts, and

help identify other locations where skimming occurred. Finally, information regarding communications and associates will help identify other, unknown conspirators. In particular, HORNEA's description of the mechanic, communications with others, and even his requests to others for equipment, demonstrate that there remain other, unidentified conspirators. I believe that this information will help identify those people and, in the case of the mechanic, provide more than a nickname.

72. Subscriber information regarding the Facebook Accounts is also relevant to show ownership and control of the Accounts. In addition, such information, with regard to the LUDEMIS HORNEA Facebook Account, will show that HORNEA also used the Device both in furtherance of the Target Offenses and to access the account.

73. Based on my training and experience, I am aware that criminals, especially criminals who use computers to facilitate their criminal activity, use social media or communicate with others over the internet, and often use Facebook and other messaging features to communicate with others about their criminal conduct, as is already demonstrated above.

74. On July 6, 2016, a request was submitted under 18 U.S.C. § 2703(f) via the Facebook law enforcement portal that the company preserve all records associated with the Facebook Accounts (except for the BADEA Facebook Account). Facebook indicates that it will preserve these records through December 3, 2016.

75. From my training and experience, I am aware that companies that host social-networking accounts, and Facebook in particular, generally maintain records of their subscribers' online activities and private communications unless the user deletes these communications.

***LEGAL AUTHORITY***

76. The government may obtain both electronic communications and subscriber

information by obtaining a search warrant. 18 U.S.C. §§ 2703(a), 2703(c)(1)(A).

77. Any court with jurisdiction over the offense under investigation may issue a search warrant under 18 U.S.C. § 2703(a), regardless of the location of the Internet company whose information will be searched. 18 U.S.C. § 2703(b)(1)(A). Furthermore, unlike other search warrants, § 2703 warrants do not require an officer to be present for service or execution of the search warrant. 18 U.S.C. § 2703(g).

78. If the government obtains a search warrant, there is no requirement that either the government or the provider give notice to the subscriber. 18 U.S.C. §§ 2703(b)(1)(A), 2703(c)(3).

***REQUEST TO SEAL AND PRECLUDE NOTICE TO THE SUBSCRIBER***

79. I request that this application, the warrant, the order, and any related papers be sealed by the Court until such time as the Court directs otherwise, except that the United States may later produce copies of the search warrant and related documents to the defense during discovery in any criminal case. I further request that, pursuant to 18 U.S.C. §§ 2705(b) and 2703(b)(1)(A), the Court order Facebook and Google not to notify any person (including the subscribers or customers to which the materials relate) of the existence of this application, the warrant, or the execution of the warrant. Such an order is justified because notification of the application, the warrant, or the execution of the warrant could seriously jeopardize the ongoing investigation by giving the subscriber notice of the investigation and an opportunity to destroy evidence, notify confederates, intimidate witnesses, or flee from prosecution.

80. The government will notify Facebook and Google within 30 days of the conclusion of the criminal investigation described in the application, unless such period is extended by the court in accordance with § 2705(b). After such notification, Facebook and

Google shall no longer be bound by the nondisclosure order. Facebook and Google may also inquire with the government about whether non-disclosure is still necessary, and the government shall respond promptly to such inquiries.

***FOURTEEN-DAY RULE FOR EXECUTION OF THE WARRANT***

81. Federal Rule of Criminal Procedure 41(e)(2)(A),(B) directs the United States to execute a search warrant for electronic evidence within 14 days of the warrant's issuance. If the Court issues this warrant, the United States will execute it not by entering the premises of Facebook, as with a conventional warrant, but rather by serving a copy of the warrant on the companies and awaiting their production of the requested data. This practice is approved in 18 U.S.C. § 2703(g), and it is generally a prudent one because it minimizes the government's intrusion onto Internet companies' physical premises and the resulting disruption of their business practices.

82. Based on the training and experience of myself and other law enforcement, I understand that e-mail and social media providers sometimes produce data in response to a search warrant outside the 14-day (formerly 10-day) period set forth in Rule 41 for execution of a warrant. I also understand that electronic communication companies sometimes produce data that was created or received after this 14-day deadline ("late-created data"). The United States does not ask for this extra data or participate in its production.

83. Should Facebook or Google produce late-created data in response to this warrant, law enforcement personnel will seek to avoid reviewing any late-created data that was created by or received by the account-holder(s) absent a follow-up warrant. However, I request permission to view all late-created data that was created by Facebook, including subscriber, IP address, logging, and other transactional data, without a further order of the Court. This information

could also be obtained by grand jury subpoena or an order under 18 U.S.C. § 2703(d), neither of which contains a 14-day time limit.

84. For these reasons, I request that the Court approve the procedures in the respective Attachments B, which set forth these limitations.

***CONCLUSION***

85. Based on the information described above, I have probable cause to believe that HORNEA and others have committed the Target Offenses.

86. Based on the information described above, there is probable cause to believe that the Facebook Accounts (as described in Attachment A) contains fruits, evidence, and instrumentalities of these crimes (as described in Attachment C). The procedures for copying and reviewing the relevant records are set out in Attachment C.

87. Based on the information described above, I have probable cause to believe that records and data from the Target Google Accounts (as described in Attachment B), contain evidence, fruits, and instrumentalities of the above-listed crimes (as described in Attachment D). The procedures for copying and reviewing the relevant records are set out in Attachment D to the search warrant.

Sworn to under the pains and penalties of perjury.

JASON D. COSTELLO
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me on August 26, 2016.

DONALD L. CABELL
United Sates Magistrate Judge

**ATTACHMENT A-FACEBOOK**

The premises to be searched and seized are (1) the Facebook accounts associated with

a. the Facebook user identification ("UID") 100004369117504 and vanity uniform resource locator ("URL") of www.facebook.com/ludemis.hornea ("the LUDEMIS HORNEA Facebook Account")

b. the Facebook UID 100004495770593 (the "CONSTANTIN HORNEA Facebook Account") and URL www.facebook.com/profile.php?id=100004495770593;

c. the Facebook UID 100000309485302 and Vanity URL www.facebook.com/claudio.florea (the "CLAUDIU Facebook Account");

d. the Facebook UID 100006871982416 and Vanity URL www.facebook.com/ludy.ludemis.9 ("LUDY LUDEMIS Facebook Account");

e. the Facebook UID 100004680823873 and Vanity URL www.facebook.com/stau.cavulturupestaca ("SUEDIN CHICIU Facebook Account");

f. the Facebook UID 100001843243076 and Vanity URL www.facebook.com/chdheu ("BADEA Facebook Account"); and

g. the Facebook UID 100003187275603 and Vanity URL www.facebook.com/birgu.boss ("BIRGU BOSS Facebook Account," collectively the "Facebook Accounts").

(2) other user-generated data stored with the Facebook Accounts; and (3) associated subscriber, transactional, and user connection information associated with the Facebook Accounts, as described further in Attachment C. This information is maintained by Facebook, Inc., which accepts service of process at 1601 Willow Road, Menlo Park, CA 94025 and via its law enforcement portal at www.facebook.com/records.

**ATTACHMENT B-GOOGLE**

The premises to be searched and seized are (1) the e-mail accounts identified as ludy.ludemis@gmail.com and ludemis.hornea@gmail.com (the "Target Google Accounts"), (2) other user-generated data stored with those accounts, and (3) associated subscriber, transactional, user connection information associated with the accounts, as described further in Attachment D. This information is maintained by Google, which accepts service of process at: USLawEnforcement@google.com and via its law enforcement portal at https://support.google.com/legal-investigations/contact/LERS.

## ATTACHMENT C-FACEBOOK

### I. Search Procedure

A. Within fourteen days of the search warrant's issue, the warrant will be served on Facebook personnel, who will identify the accounts and files to be searched, as described in Section II below.

B. The company will then create an exact electronic duplicate of these accounts and files ("the account duplicate").

C. The company will provide the account duplicate to law enforcement personnel.

D. Law enforcement personnel will then search the account duplicate for the records and data to be seized, which are described in Section III below.

E. Law enforcement personnel may review the account duplicate, even if the company produced it after fourteen days from the warrant's issue, subject to the following limitations. If the company provided data that was created after fourteen days from the warrant's issue ("late-created data"), law enforcement personnel may view all late-created data that was created by the company, including subscriber, IP address, logging, and other transactional data, without a further order of the Court. Law enforcement personnel will seek to avoid reviewing any late-created data that was created by or received by the account-holder(s), such as e-mail, absent a follow-up warrant.

### II. Accounts and Files to Be Copied by Company Personnel

A. All data files associated with the account associated with,

a. the Facebook user identification ("UID") 100004369117504 and vanity uniform resource locator ("URL") of www.facebook.com/ludemis.hornea ("the LUDEMIS HORNEA Facebook Account")

b. the Facebook UID 100004495770593 (the "CONSTANTIN HORNEA Facebook Account") and URL www.facebook.com/profile.php?id=100004495770593;

c. the Facebook UID 100000309485302 and Vanity URL www.facebook.com/claudio.florea (the "CLAUDIU Facebook Account");

d. the Facebook UID 100006871982416 and Vanity URL www.facebook.com/ludy.ludemis.9 ("LUDY LUDEMIS Facebook Account");

e. the Facebook UID 100004680823873 and Vanity URL www.facebook.com/stau.cavulturupestaca ("SUEDIN CHICIU Facebook Account");

f. the Facebook UID 100001843243076 and Vanity URL www.facebook.com/chdheu ("BADEA Facebook Account"); and

g. the Facebook UID 100003187275603 and Vanity URL www.facebook.com/birgu.boss ("BIRGU BOSS Facebook Account," collectively the "Facebook Accounts").

including any materials preserved on July 6, 2016, when the preservation request was initiated on this account, in the following categories:

1. Biographical profile information entered by the user, including data characterized by Facebook, in the following categories:

   - "About Me";
   - "Date of Birth";
   - "Education";
   - "Favorite Quotes";

- "Gender";
- "Hometown";
- "Physical Tokens" ("Badges" added by the user to the account);
- "Work".

2. Information regarding the user's activities on Facebook and on pages with Facebook connections visited while connected to Facebook, including data characterized by Facebook in the following categories:

   - "Ads Clicked";
   - "Ad Topics";
   - "Apps" subscribed to;
   - "Likes on Other Sites";
   - "Privacy Settings"
   - "Recent Activities";
   - "Searches";
   - Web pages visited that have a Facebook "Like" button;

3. Communications and messages published, sent or received by the user, including data characterized by Facebook in the following categories:

   - "Chat";
   - "Messages";
   - "Notes;"
   - "Photos";
   - "Your Posts";
   - "Posts By Others";
   - "Shares";

- "Status Updates";
- "Videos"

4. Information about the user's associates, including data characterized by Facebook in the following categories:

   - "Connections";
   - "Deleted Friends";
   - "Family";
   - "Followers";
   - "Following";
   - "Friend Requests";
   - "Friends";
   - "Groups";
   - "Hidden from News Feed" (Friends, apps, or pages hidden from news feed);
   - "Likes on Other's Posts";
   - "Likes on Your Posts from others";
   - "Networks";
   - "Pending Friend Requests";
   - "Photos";
   - "Pokes";
   - "Removed Friends";
   - "Tag Suggestions Template" (used to help friends "tag" the user in photos that are uploaded

5. Information regarding the user's location and movements, including data characterized by Facebook in the following categories:

- "Check-ins";
- "Current City";
- "Events";
- "Last Location";
- "Locale";
- "Photos Metadata" (EXIF);

B. All subscriber and transactional records for this account and any associated accounts, including Instagram accounts linked to this account:

1. Names, including;
   - "Name"
   - "Alternate Name"
   - "Name Changes"
   - "Screen Names"
   - "Vanity URL"
2. Addresses, including;
   - "Address"
   - "Emails" (addresses, including removed addresses)
   - "IP Addresses"
3. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions, including;
   - "Active Sessions"
   - "Logins"
   - "Logouts"

4. Length of service and types of service utilized, including;

- "Account Status History"
- "Registration Date"
- "Notification Settings";
- "Privacy Settings";
- List of Types of Facebook services utilized (e.g. , "Messages," "Notes")

5. Telephone or instrument numbers, including;

- "Phone Numbers"

6. Other subscriber numbers or identities, including;

- "Pages You Admin"
- "Linked Accounts"

7. Means and source of payment, including;

- "Credit Cards"
- "Currency"

**III. Records and Data to be Searched and Seized by Law Enforcement Personnel**

A. Evidence, fruits, and instrumentalities of conspiracy to use counterfeit access devices in violation of 18 U.S.C. § 1029(b)(2) and possession of device making equipment in violation of 18 U.S.C. § 1029(a)(4) (hereinafter, the "Target Offenses"), including records or data relating to:

1. Communications or other information relating to skimming, counterfeit access devices or device making equipment, including the sources of equipment and target ATMs;
2. The identity and location of any co-conspirators;

3. Computer activity in furtherance of the Target Offenses;

4. The identity and past or present location of LUDEMIS HORNEA a/k/a "Antonio Scapescia" a/k/a "Alex Velea" a/k/a "Ludy Ludemis", ION BONCULESCU a/k/a "Nutu Poescu", ISABELA FLOREA, ENTES MUSTAFA, CONSTANTIN DENIS HORNEA a/k/a "Faby Fabritio", CLAUDIU FLOREA, SUEDIN CHICIU, FERNANDO FLORIN BADEA, and any co-conspirators;

5. The identity, location, and ownership of any computers used to access the Facebook Accounts;

6. Other e-mail or Internet accounts, telephone numbers, social media services, or web or mobile based applications providing Internet access, remote data storage, or communication services for LUDEMIS HORNEA a/k/a "Antonio Scapescia" a/k/a "Alex Velea" a/k/a "Ludy Ludemis", ION BONCULESCU a/k/a "Nutu Poescu", ISABELA FLOREA, ENTES MUSTAFA, CONSTANTIN DENIS HORNEA a/k/a "Faby Fabritio", CLAUDIU FLOREA, SUEDIN CHICIU, FERNANDO FLORIN BADEA, or co-conspirators;

7. The sources of income, and the location of, and identifiers for, bank accounts, e-currency accounts, and credit accounts for LUDEMIS HORNEA a/k/a "Antonio Scapescia" a/k/a "Alex Velea" a/k/a "Ludy Ludemis", ION BONCULESCU a/k/a "Nutu Poescu", ISABELA FLOREA, ENTES MUSTAFA, CONSTANTIN DENIS HORNEA a/k/a

"Faby Fabritio", CLAUDIU FLOREA, SUEDIN CHICIU, FERNANDO FLORIN BADEA, or co-conspirators;

B. All of the subscriber, transactional, and logging records described in Section II (B).

## ATTACHMENT D-GOOGLE

**I. Search Procedure**

A. Within fourteen days of the search warrant's issue, the warrant will be served on Google, which will identify the accounts and files to be searched, as described in Section II below.

B. Google will then create an exact electronic duplicate of these accounts and files ("the account duplicate").

C. Google will provide the account duplicate to law enforcement personnel.

D. Law enforcement personnel will then search the account duplicate for the records and data to be seized, which are described in Section III below.

E. Law enforcement personnel may review the account duplicate, even if it is produced more than 14 days after the warrant issues, subject to the following limitations. If data was created after fourteen days from the warrant's issue ("late-created data") law enforcement personnel may view all late-created data, including subscriber, IP address, logging, and other transactional data, without a further order of the Court. Law enforcement personnel will seek to avoid reviewing any late-created data that was created by or received by the account-holder(s), absent a follow-up warrant.

**II. Accounts and Files to Be Copied by Google Personnel**

A. All data files associated with the Target Google Accounts, including:

1. The contents of all e-mail, whether draft, deleted, sent, or received;

2. The contents of all text or instant messages;

3. The contents of all electronic data files, whether word-processing, spreadsheet, image, video, or any other content;

4. The contents of all calendar data;

5. Lists of friends, buddies, contacts, or other subscribers;

6. Records pertaining to communications between Google and any person regarding these accounts and any e-mail accounts associated with those addresses, including, without limitation, contacts with support services and records of actions taken.

B. All subscriber and transactional records for the Target Google Accounts and any associated e-mail accounts, including:

1. Subscriber information for these and any associated e-mail accounts:

   a. Name(s) and account identifiers;

   b. Address(es);

   c. Records of session times and durations;

   d. Length of service (including start date) and types of service utilized;

   e. Telephone instrument number of other subscriber number or identity, including any temporary assigned network address;

   f. The means and source of payment for such service (including any credit card or bank account number); and

   g. The Internet Protocol address used by the subscriber to register the account or otherwise initiate service.

2. User connection logs for any connections to or from these and any associated e-mail accounts, including:

a. Connection time and date;

b. Disconnect time and date;

c. The IP address that was used when the user connected to the service;

d. Source and destination of any e-mail messages sent from or received by the account, and the date, time, and length of the message; and

e. Any address to which e-mail was or is to be forwarded from the account or e-mail address.

3. Any connection logs or user logs and all stored data pertaining to the following services: Google Calendar, Google Photos, Google Maps, Google Hangouts, Location History, and Web History for the period January 1, 2015 to the present.

## III. Records and Data to be Searched and Seized by Law Enforcement Personnel

A. Evidence, fruits, or instrumentalities of conspiracy to use counterfeit access devices in violation of 18 U.S.C. § 1029(b)(2) and possession of device making equipment in violation of 18 U.S.C. § 1029(a)(4) (hereinafter, the "Target Offenses"), relating to:

1. All communications between or among LUDEMIS HORNEA a/k/a "Antonio Scapescia" a/k/a "Alex Velea" a/k/a "Ludy Ludemis", ION BONCULESCU a/k/a "Nutu Poescu", ISABELA FLOREA, ENTES

MUSTAFA, CONSTANTIN DENIS HORNEA a/k/a “Faby Fabritio”, CLAUDIU FLOREA, SUEDIN CHICIU, FERNANDO FLORIN BADEA, or co-conspirators;

2. All communications pertaining to LUDEMIS HORNEA a/k/a “Antonio Scapescia” a/k/a “Alex Velea” a/k/a “Ludy Ludemis”, ION BONCULESCU a/k/a “Nutu Poescu”, ISABELA FLOREA, ENTES MUSTAFA, CONSTANTIN DENIS HORNEA a/k/a “Faby Fabritio”, CLAUDIU FLOREA, SUEDIN CHICIU, FERNANDO FLORIN BADEA, or co-conspirators;
3. The identity of the person or persons who have owned or operated the Target Google Accounts or any associated e-mail accounts;
4. The contents of all electronic data files, whether word-processing, spreadsheet, image, video, or any other content;
5. The contents of all calendar data;
6. Lists of friends, buddies, contacts, or other subscribers;
7. The existence and identity of any co-conspirators;
8. The travel or whereabouts of the person or persons who have owned or operated the Target Google Accounts or any associated e-mail accounts;
9. The identity, location, and ownership of any computers used to access these e-mail accounts;
10. Other e-mail or Internet accounts providing Internet access or remote data storage;

11. The existence or location of physical media storing electronic data, such as hard drives, CD- or DVD-ROMs, or thumb drives; and

12. The existence or location of paper print-outs of any data from any of the above.

B. All of the subscriber, transactional, and logging records described in Section II(B).